FIG.1

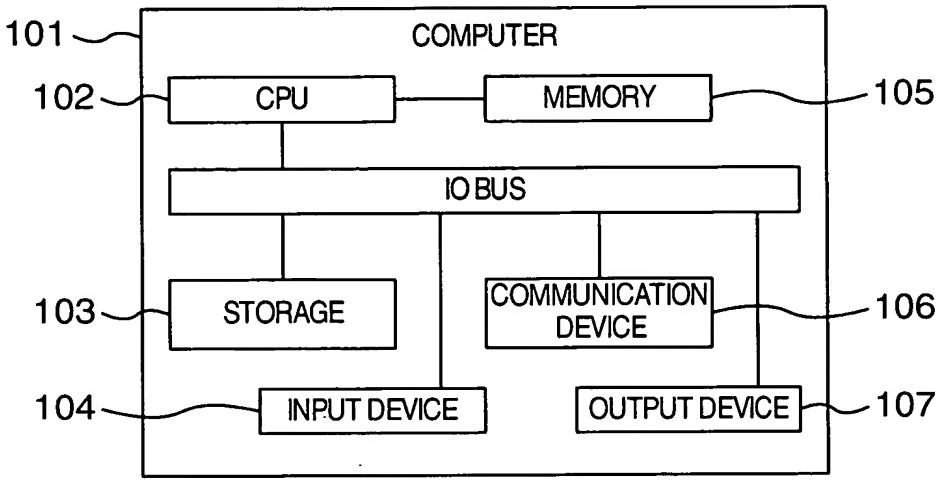


FIG.2

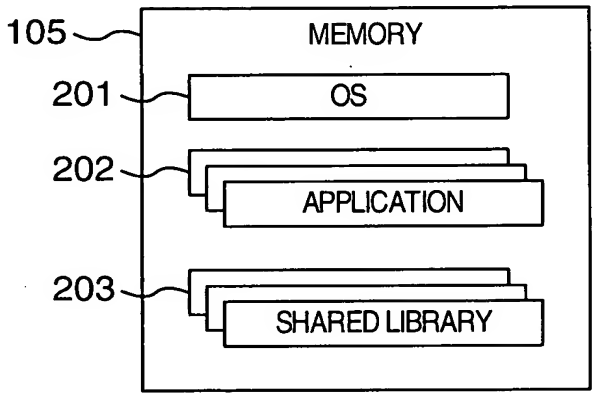


FIG.3

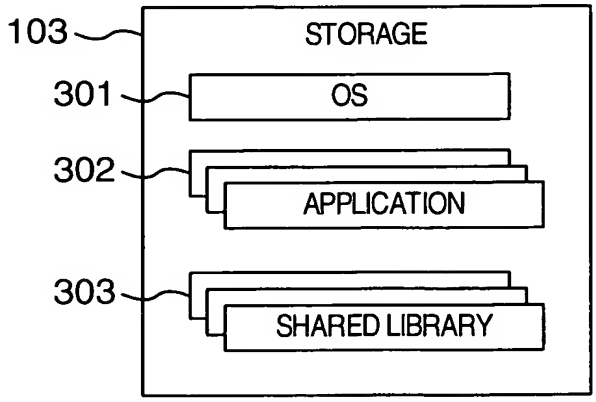


FIG.4
PRIOR ART

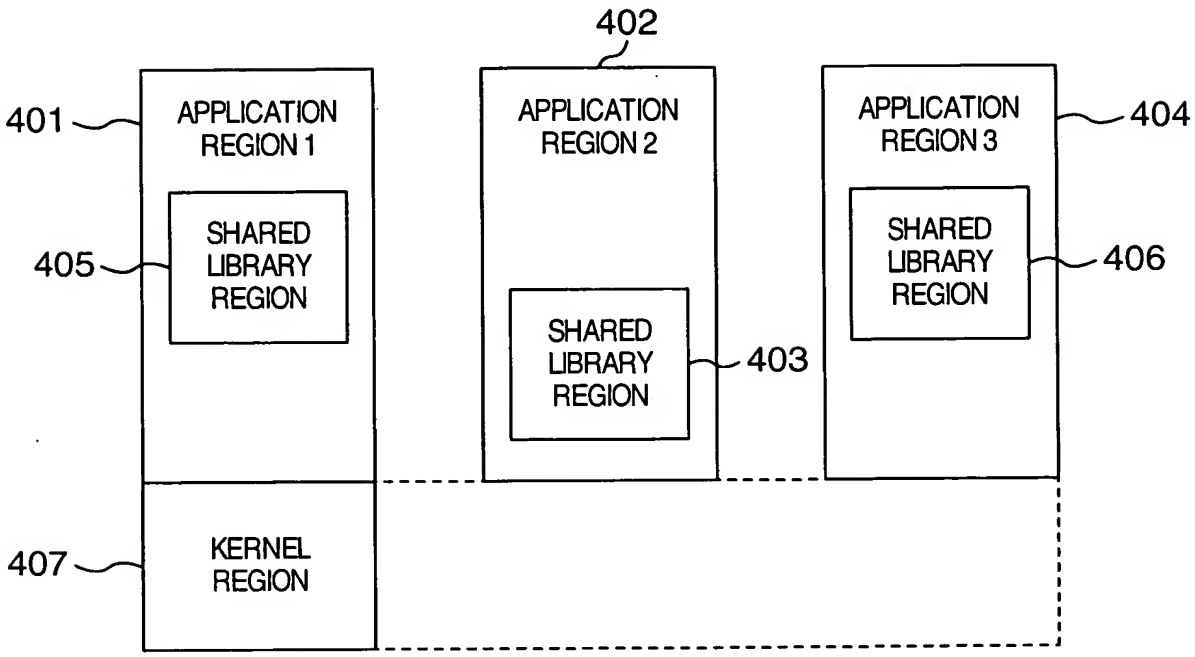


FIG.5
PRIOR ART

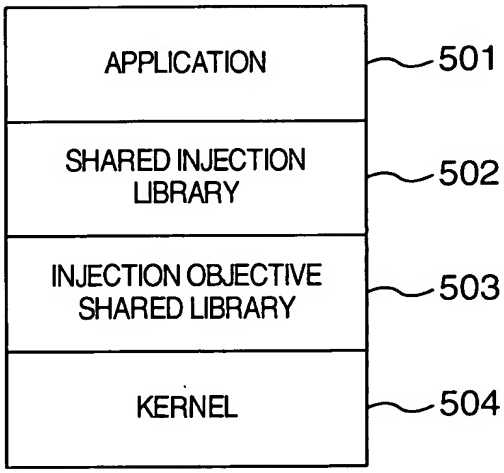


FIG.6

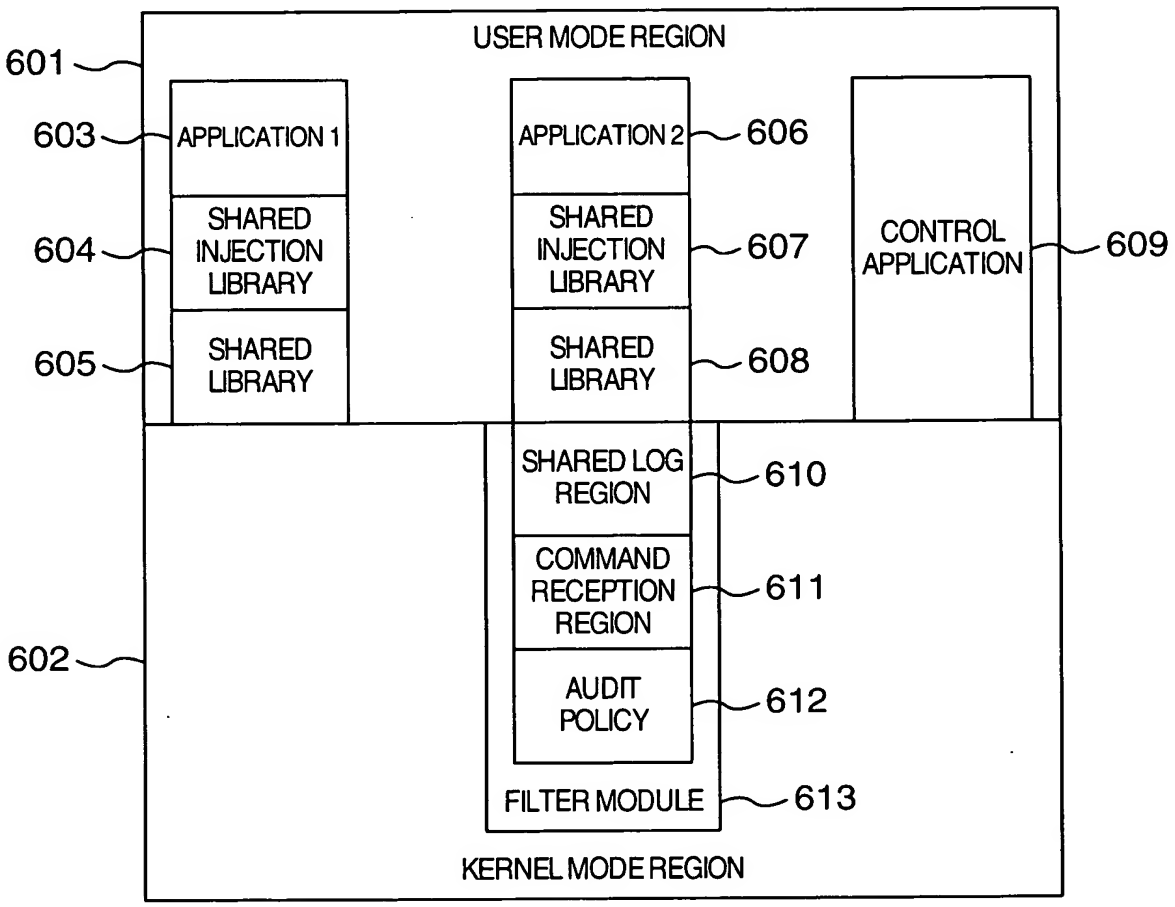

USER MODE REGION
601
603
APPLICATION 1
604
SHARED INJECTION LIBRARY
605
SHARED LIBRARY
APPLICATION 2
606
SHARED INJECTION LIBRARY
607
SHARED LIBRARY
608
CONTROL APPLICATION
609
SHARED LOG REGION
610
COMMAND RECEPTION REGION
611
AUDIT POLICY
612
FILTER MODULE
613
602
KERNEL MODE REGION

FIG.7

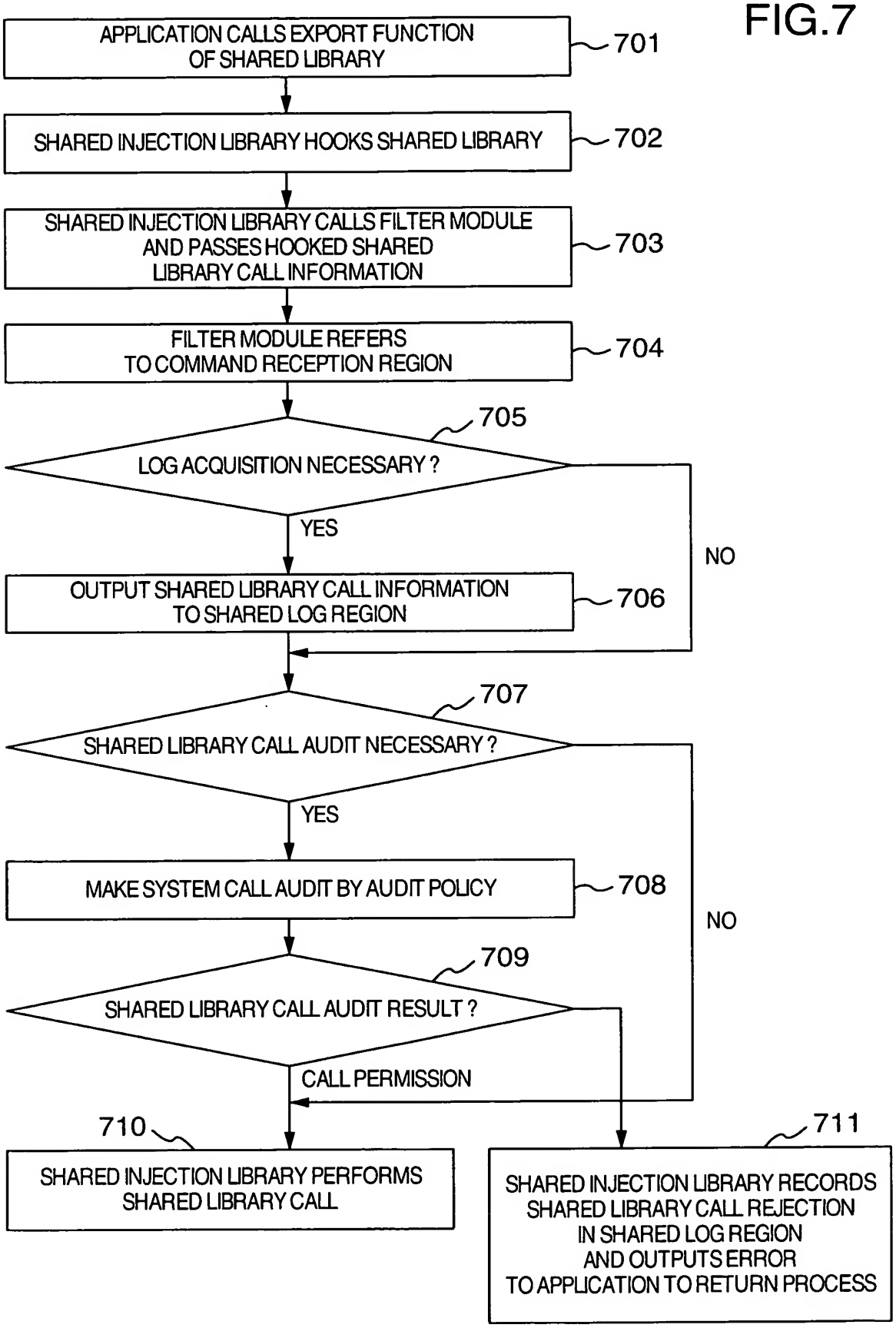

APPLICATION CALLS EXPORT FUNCTION OF SHARED LIBRARY
701
SHARED INJECTION LIBRARY HOOKS SHARED LIBRARY
702
SHARED INJECTION LIBRARY CALLS FILTER MODULE AND PASSES HOOKED SHARED LIBRARY CALL INFORMATION
703
FILTER MODULE REFERS TO COMMAND RECEPTION REGION
704
705
LOG ACQUISITION NECESSARY ?
YES
NO
OUTPUT SHARED LIBRARY CALL INFORMATION TO SHARED LOG REGION
706
707
SHARED LIBRARY CALL AUDIT NECESSARY ?
YES
NO
MAKE SYSTEM CALL AUDIT BY AUDIT POLICY
708
709
SHARED LIBRARY CALL AUDIT RESULT ?
CALL PERMISSION
710
SHARED INJECTION LIBRARY PERFORMS SHARED LIBRARY CALL
711
SHARED INJECTION LIBRARY RECORDS SHARED LIBRARY CALL REJECTION IN SHARED LOG REGION AND OUTPUTS ERROR TO APPLICATION TO RETURN PROCESS

FIG.8

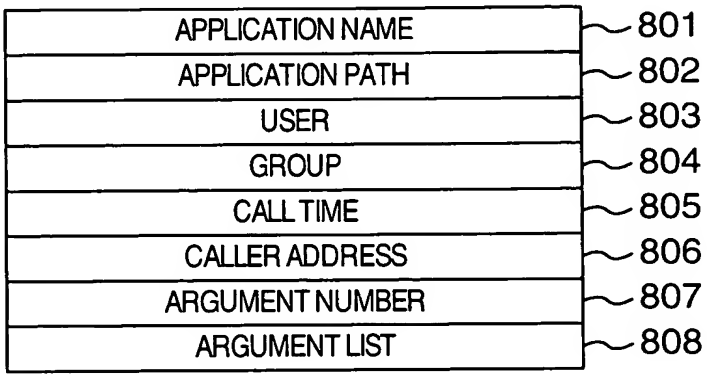


FIG.9

901 FUNCTION NAME	902 APPLICATION NAME	903 APPLICATION PATH	904 USER	905 GROUP	906 PERMISSION TIME	907 PERMISSION ADDRESS	908 ARGUMENT AUDIT CONTENT	909
open	App 1	/bin/	User 1	Grp 1	8:00 - 17:00	-7000000		910
open	App 2	/usr/bin/	User 2	Grp 2	24h	2000 - 4000		911
close	App 3	/var/bin/	User 3	Grp 3	17:00 - 0:00	80000000 -		912

FIG.10

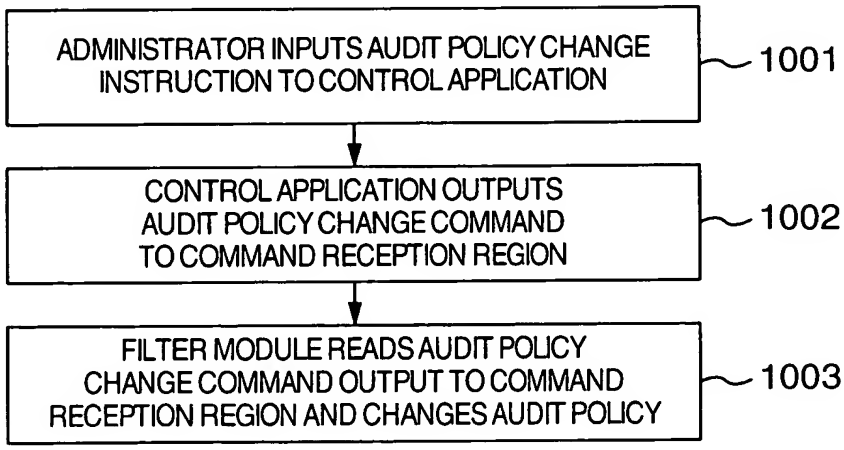
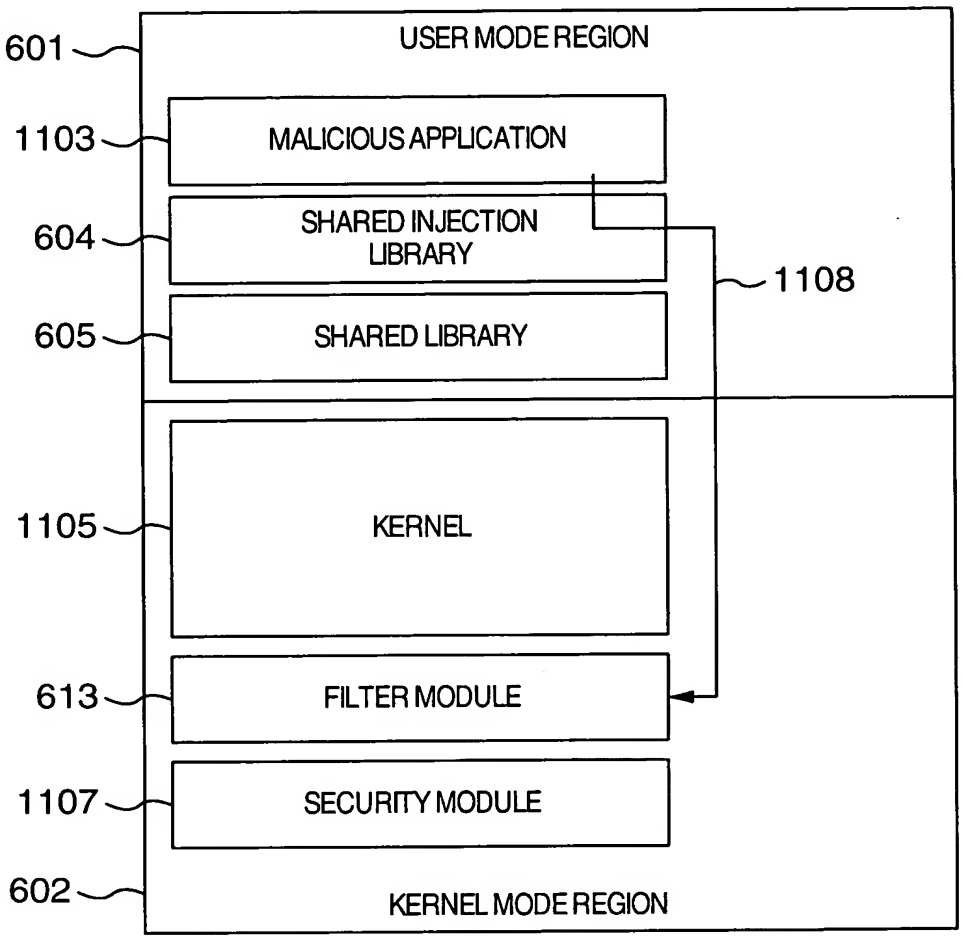


FIG.11


601
USER MODE REGION
1103
MALICIOUS APPLICATION
604
SHARED INJECTION LIBRARY
1108
605
SHARED LIBRARY
1105
KERNEL
613
FILTER MODULE
1107
SECURITY MODULE
602
KERNEL MODE REGION